Regione Emilia-Romagna
Assemblea Legislativa

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

LIBRI E CONVERSAZIONI

Incontri con autori ed esperti,
a cura della biblioteca dell'Assemblea legislativa della Regione Emilia-Romagna
e delle biblioteche giuridiche dell'Università di Bologna

FIRME ELETTRONICHE ED EFFICACIA GIURIDICA

BOLOGNA, 12 DICEMBRE 2011 ORE 10.30/13.00

BIBLIOTECA DELL'ASSEMBLEA LEGISLATIVA - REGIONE EMILIA-ROMAGNA - VIALE ALDO MORO, 32

INTERVENGONO

MONICA PALMIRANI - MICHELE MARTONI
ANNA VOLTAN - ANNA FIORENZA

Grafica: Roberta Gravano, *Centro grafico dell'Assemblea* - Stampa: Centro stampa regionale

Approccio innovativo e interdisciplinare

*se vuoi viaggiare **veloce***
viaggia da solo
*ma se vuoi andare **lontano***
viaggia in compagnia

(proverbio africano)

Innovazione? presente!

quando il tempo è maturo
per certe cose
queste appaiono in diversi luoghi
proprio come le violette
sbocciano dappertutto
quando comincia la primavera

(Farkas Bolyai, 1830, matematico)

firme elettroniche *e* **identità**

Constatazione: Rete “reale” *non* virtuale

- Popolazione mondiale

  6 miliardi 900 milioni

  (Istituto francese di studi demografici, agosto 2011)

- Utenti Internet nel mondo

  2 miliardi 100 milioni

  (Internet World Stats, marzo 2011)

- Utenti Facebook

  800 milioni (350 milioni by mobile)

  (Facebook, dicembre 2011)

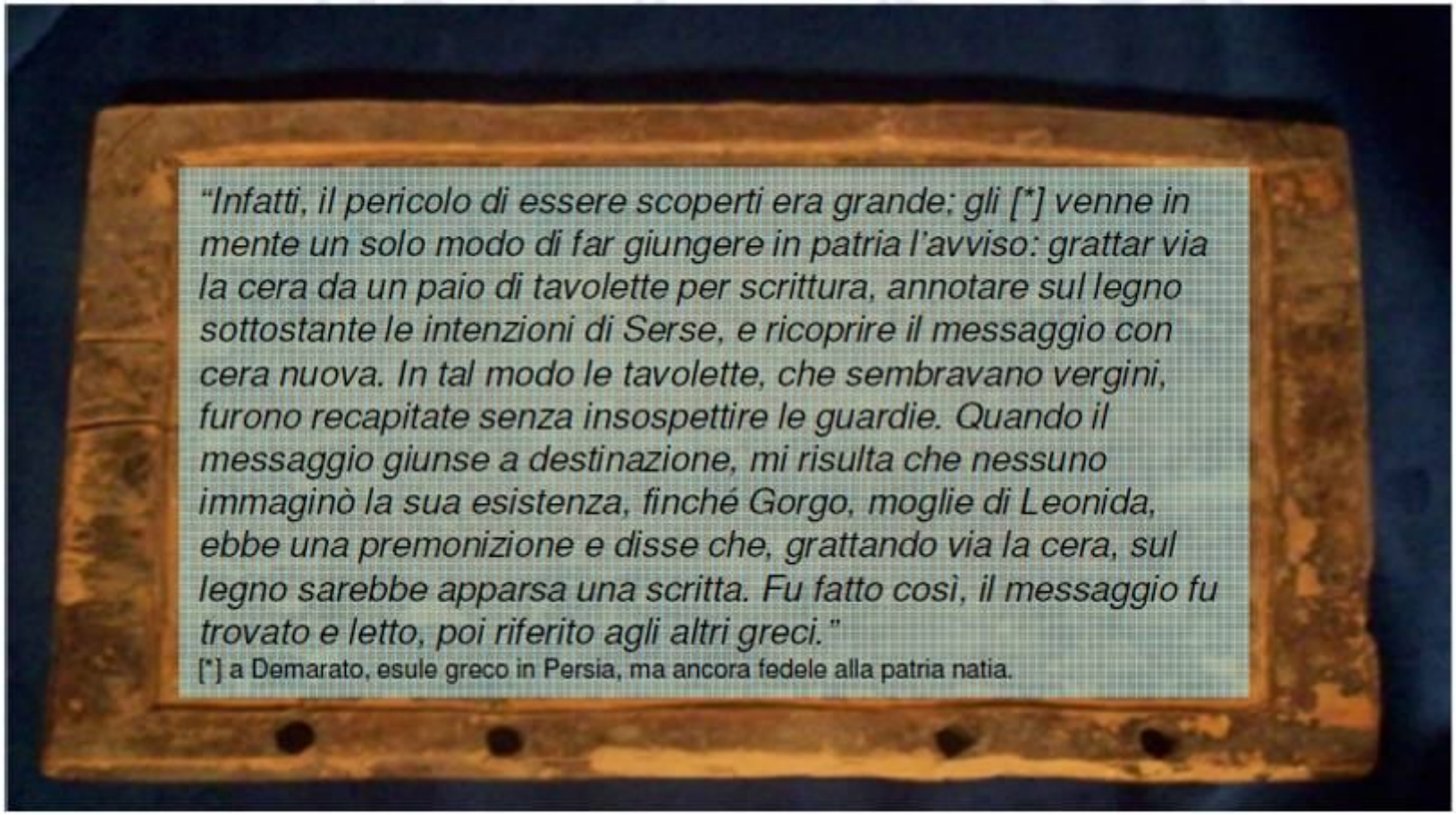
firme elettroniche *e* **identità**

Quesito 1)
Come posso attestare la mia identità in rete? E verificare quella del mio interlocutore?

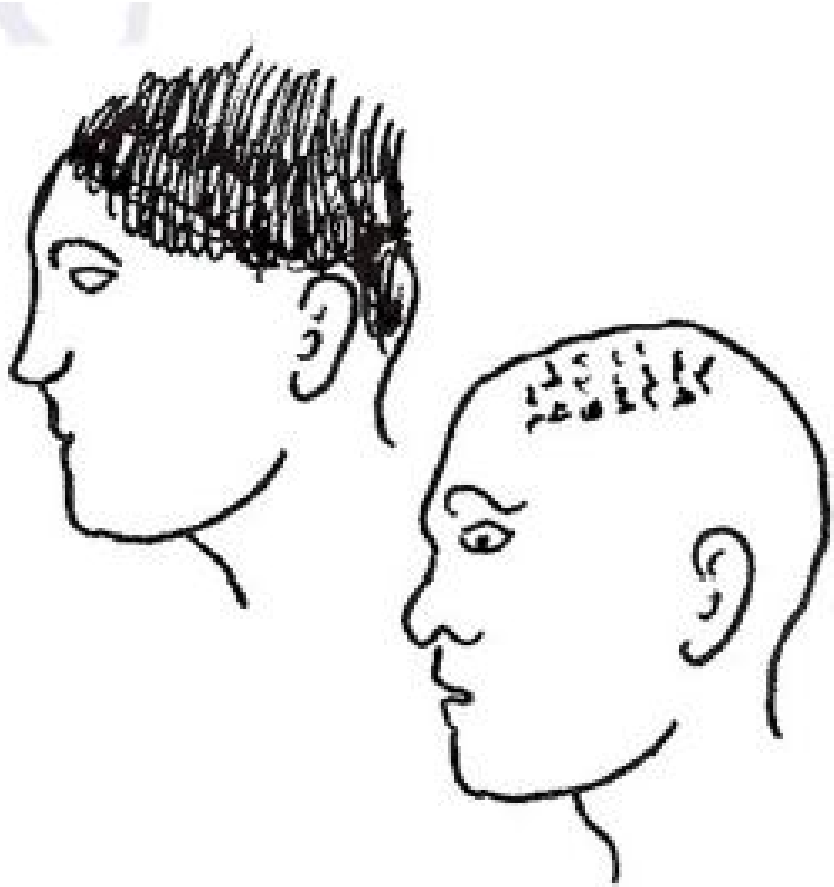
Quesito 2)
Come posso tutelare la segretezza e l'integrità delle mie comunicazioni elettroniche?

un’epoca un sistema

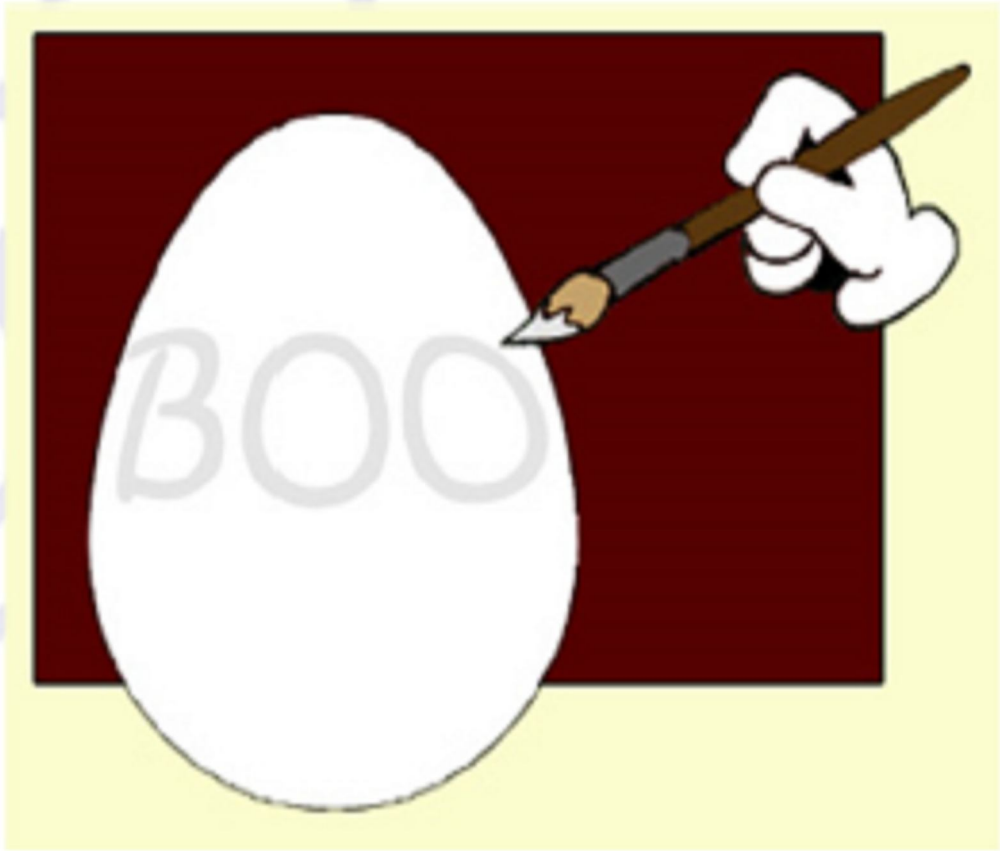
- Steganografia
  - Occultamento **fisico** del messaggio
    - Il messaggio è “invisibile”
    - Intercettazione: forte rischio di pregiudizio



(Immagini tratte da http://avires.dimi.uniud.it/claudio/teach/sicurezza2011/lezione-01.pdf)



(Immagini tratte da http://avires.dimi.uniud.it/claudio/teach/sicurezza2011/lezione-01.pdf)



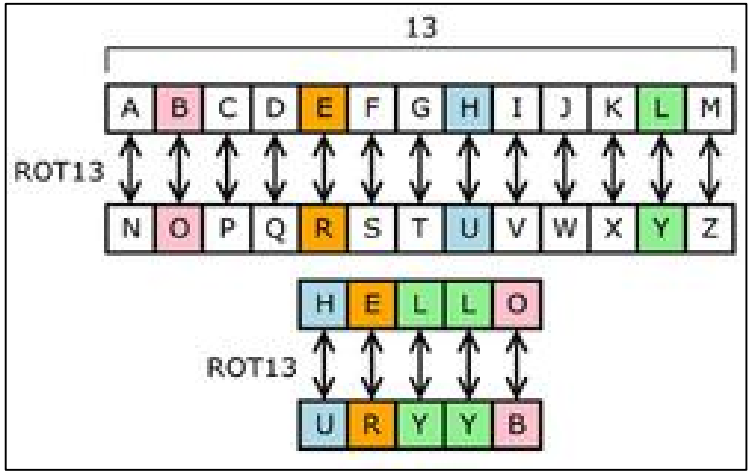
(Immagini tratte da http://avires.dimi.uniud.it/claudio/teach/sicurezza2011/lezione-01.pdf)

un’epoca un sistema

- Crittografia
  - Occultamento **semantico** del contenuto del messaggio
    - Il messaggio è “visibile” ma non “comprensibile”
    - Key management

Metodo Traspositivo

Spostamento di Cesare



Metodo Sostitutivo

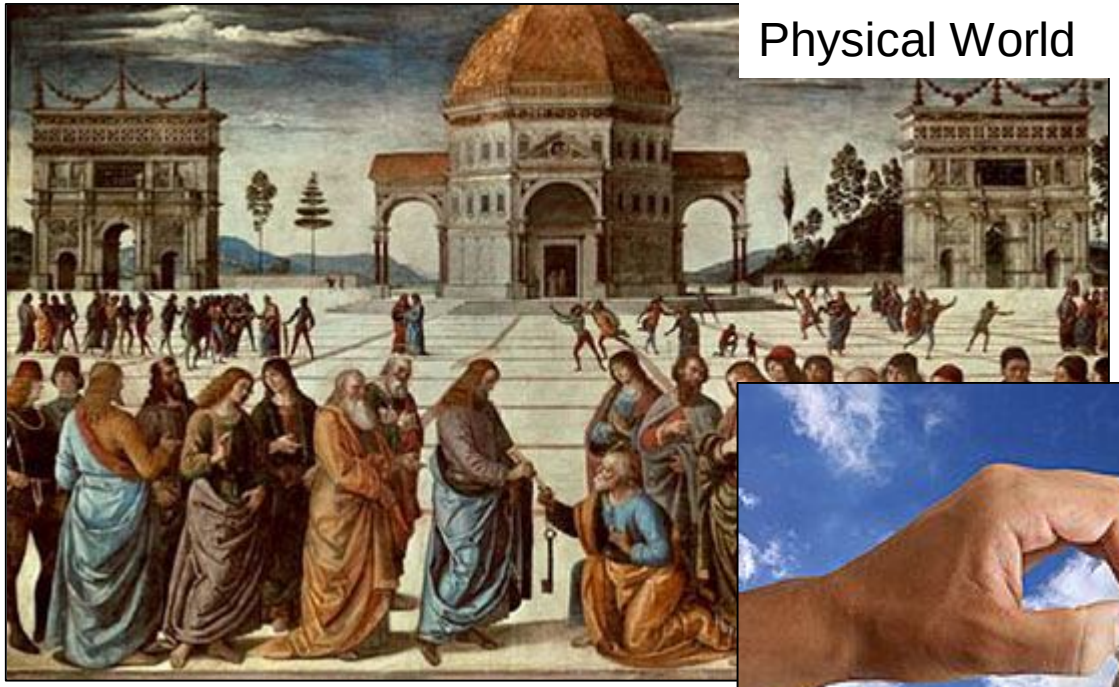
Disco cifrante di Alberti

crittografia simmetrica
crittografia asimmetrica

- La **crittografia simmetrica**, nota anche come crittografia a **chiave privata** o a **chiave segreta**, è quella particolare tecnica crittografica che prevede l'utilizzo di un’unica chiave sia per l'operazione di cifratura sia per quella di decifratura

Here is a fine example of a pre-WWII built Luftwaffe Enigma machine (serial A6345 dated 1937) with the added benefit of three high-quality, matched, rotors and the Umkehrwalze D option. The German designation is Chiffriermaschine Gesellschaft and it was made by Heimsoeth und Rinke of Berlin. (Photo courtesy John Alexander, G7GCK Leicester, England.

key exchange



Physical World

Web

Diffie Hellman Merkle

Stanford 1976

Diffie, Hellman, Merkle

Rivest Shamir Adleman

MIT 1977

Shamir, Rivest, Adleman

crittografia simmetrica
crittografia asimmetrica

- La **crittografia asimmetrica** (crittografia **a doppia chiave** o **crittografia a chiave pubblica**) contempla invece l'impiego di una coppia di chiavi, **una chiave pubblica ed una chiave privata**. Il principio sotteso a questa particolare tecnica prevede che quanto viene cifrato con una chiave potrà essere decifrato esclusivamente con l'altra chiave della coppia

Crittografia asimmetrica

Una chiave **(K_{PRIV})** per cifrare

Un’altra chiave **(K_{PUB})** per decifrare

Due chiave diverse ma correlate (K_{PRIV} K_{PUB})

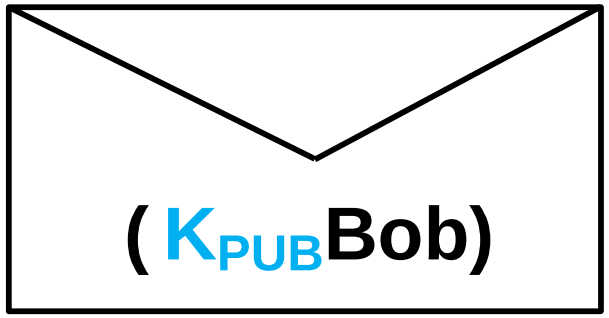
1. **Chiave privata (K_{PRIV})** conosciuta solo dal titolare
2. **Chiave pubblica (K_{PUB})** conosciuta da tutti

Testo “non firmato” e “segretato”

Alice

(K_{PUB}Alice)

(K_{PRIV}Alice)



Bob

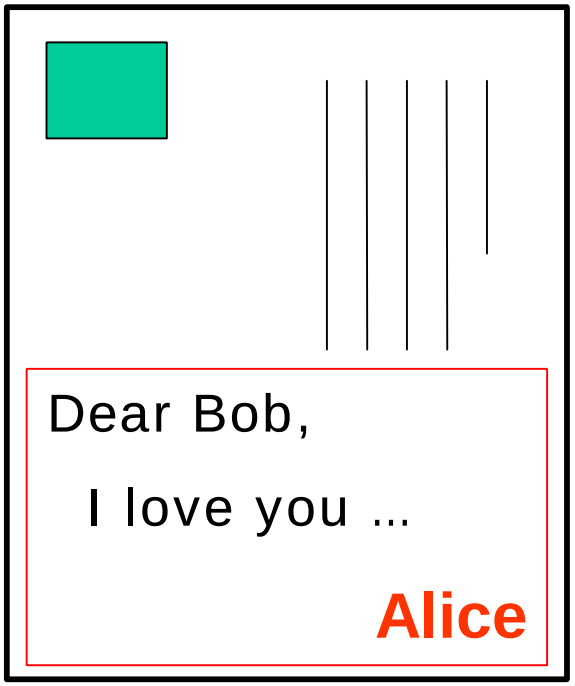
(K_{PUB}Bob)

(K_{PRIV}Bob)

- **Sicurezza/Segretezza** del contenuto **[SÌ]**
- **Autenticazione/Paternità [NO]**

Testo “firmato” e “in chiaro”

(K_{PRIV}Alice)



Alice

(K_{PUB}Alice)

(K_{PRIV}Alice)

Bob

(K_{PUB}Bob)

(K_{PRIV}Bob)

- **Sicurezza/Segretezza** del contenuto **[NO]**
- **Autenticazione/Paternità [SÌ]**

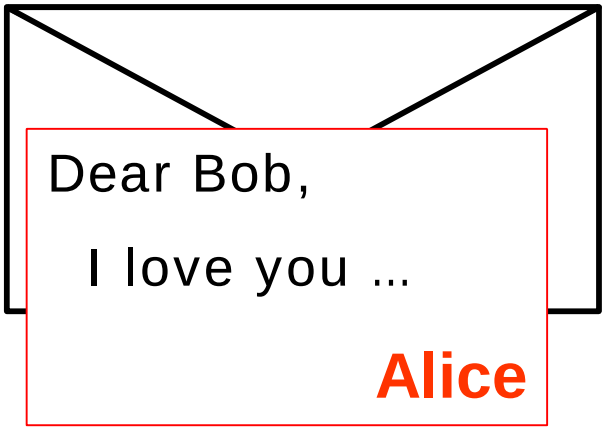
Testo “firmato” e “segretato”

(K_{PRIV}Alice)
(K_{PUB}Bob)

Alice

(K_{PUB}Alice)

(K_{PRIV}Alice)



Bob

(K_{PUB}Bob)

(K_{PRIV}Bob)

- **Sicurezza/Segretezza** del contenuto **[SÌ]**
- **Autenticazione/Paternità [SÌ]**

tempo di calcolo

hash function

Una **funzione matematica** che genera, a partire da una generica sequenza di simboli binari (*bit*), una **impronta** in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (*bit*) per le quali la funzione generi impronte uguali ...

(cfr. d.p.c.m. 30 marzo 2009)


CryptoKids®
America's Future Codemakers & Codebreakers

ex facto oritur jus

dalla crittografia alle firme elettroniche

- in principio era “solo” la **Firma digitale** 1997
- poi giunsero le **Firme elettroniche** 1999-2000

dalla crittografia alle firme elettroniche

- La firma digitale altro non è che l'**applicazione** di un **sistema di cifratura** a chiave asimmetrica

- Oltre al piano software **vi è un livello organizzativo** che unisce allo strumento di firma l'elemento della **certificazione** della identità della persona titolare dello strumento.

firma elettronica

- l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica

firma elettronica avanzata – FEA

- insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

firma elettronica qualificata

- un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

firma digitale

- un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

documento informatico

- **Documento informatico**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

documento analogico

- **Documento analogico**: la rappresentazione *non informatica* di atti, fatti o dati giuridicamente rilevanti

copie

- **copia informatica di documento analogico**: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
- **copia per immagine su supporto informatico di documento analogico**: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto

copia e duplicato

- **copia informatica di documento informatico**: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;
- **duplicato informatico**: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

Efficacia del documento informatico

Art. 20, c.1.bis

- *L'idoneità* del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio **sono liberamente valutabili in giudizio**, tenuto conto delle sue **caratteristiche** oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

Efficacia del documento informatico sottoscritto

Art. 21, c.1

- Il documento informatico, cui è apposta **una firma elettronica**, sul **piano probatorio** è **liberamente valutabile in giudizio**, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

... segue

Art. 21, c.2

- Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, **ha l'efficacia prevista dall'articolo 2702 C.c.** L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

Art. 21, c.2.bis

- Salvo quanto previsto dall'articolo 25, le **scritture private di cui all'articolo 1350**, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

... segue

Art. 21, c.3

- L’apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso **equivale a mancata sottoscrizione**. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Documenti amministrativi informatici

Art. 23.ter, c.1 e c.2

- Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, **costituiscono informazione primaria ed originale** da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.
- I documenti costituenti atti amministrativi **con rilevanza interna al procedimento amministrativo** **sottoscritti** con firma elettronica avanzata hanno l'efficacia prevista dall'**art. 2702 del codice civile**.

... segue … le copie

Art. 23.ter, c.1 e c.2

- Le **copie su supporto informatico** di documenti formati dalla pubblica amministrazione **in origine su supporto analogico** ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro **conformità all'originale** è assicurata dal funzionario a ciò delegato nell‘ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della **firma digitale** o di altra **firma elettronica qualificata** e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l’obbligo di **conservazione** dell’originale del documento è soddisfatto con la conservazione della **copia su supporto informatico**.

... segue … il contrassegno

Art. 23.ter, c.5

- Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un **contrassegno generato elettronicamente**, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da **consentire** la **verifica automatica della conformità del documento analogico a quello informatico**.

Regione Emilia-Romagna

Trenta Pia
VIA DOMICILIO 222
40100 BOLOGNA BO

Matricola	Codice Fiscale	Luogo Nascita	Data nascita	Mese retribuzione
00000002	TRNPIA78A56A944J	BOLOGNA	16.01.1978	Marzo 2009
Categoria	Centro Di Costo	Servizio		
C1				

Inail	ANF	Nr.	Tab.	% Occupaz.	Contratto Di Lavoro	Tipo Rapporto	Assunzione	Cessazione
0000000000				100,00	COMPARTO REGIONALE	Tempo indetermin. FT	20.11.2008	01.01.2010

Voce	Descrizione	MM/AA	Imponibile	Quantità	V. Unitario	Trattenute	Competenze
0A01	Stipendio			26,00	56,4223		1.466,98
0A10	Indennità di comparto			26,00	1,7615		45,80
2080	Reperibilità ordinaria	02/09		1,00	0,8600		0,86
1070	Importo a garanzia	02/09				0,86	
1070	Importo a garanzia						500,00
4DT0	Contr. CPDEL-CPS-CS dip.	02/09				0,07	
4DT0	Contr. CPDEL-CPS-CS dip.					133,88	
4DT4	Contr. F.do Credito dip.	02/09				0,01	
4DT4	Contr. F.do Credito dip.					5,29	
84C1	Rata addiz.regionale AP					4,99	
84N1	Rata addiz. comunale AP					2,72	
84N4	Rata add. com. 30% AC					2,39	
84CZ	Residuo addiz. reg. AP		39,93				
84NQ	Acconto annuale add.comun		21,52				
84NZ	Residuo addiz. com. AP		21,78				
					Totale	179,55	2.013,64

IRPEF	Mese corrente	Detrazioni	Detr. non godute	Tax Distinta	Tax Separata	Tot. Contr. Dip.	IRPEF Netta
Imponibile	1844,19					TC -139,25	
IRPEF Lorda	-451,78	88,99				TS	-362,79

Detr. Lav. Dip.	Coniuge	Figli > 3 anni	Figli < 3 anni	F. >3 anni inab.	F. <3 anni inab.	Altri familiari	NETTO A PAGARE
		N. %	N. %	N. %	N. %	N. %	
88,99							1.471,30

Banca	IBAN	CIN	ABI	CAB	Conto Corrente

Montanti annui	Cassa pensione	INADEL	Fondo credito	CASAGIT	Previd. compl.	TFR
Imponibile AC	3127,28		3127,28			2347,16
Contributi AC	-276,76		-10,94			-143,18
Imponibile AP						
Contributi AP						

Montanti annui	IRPEF	Note:
Imponibile Fiscale	3930,04	
Imposta Lorda	-959,17	
Detrazioni	169,33	
Imposta Netta	-789,84	

Per la decodifica del timbro seguire le istruzioni all'indirizzo http://www.regione.emilia-romagna.it/TimbroDigitale/Cedolino/

(Mod. RER.2009.10)

Pag. 1/1

COMUNE DI RAVENNA

SERVIZI DEMOGRAFICI

IL BOLLO DEVE ESSERE APPLICATO ED ANNULLATO NELLA STESSA GIORNATA DI RILASCIO DEL CERTIFICATO

L'imposta di bollo non è dovuta in caso di destinazione del certificato, che deviene procedere all'esenzione ai sensi dell'art. 22 del D.P.R. 26 ottobre 1972, n. 642

RISULTANZA DI NASCITA

IL SINDACO

In conformita' alle risultanze degli atti d'ufficio

CERTIFICA CHE:

risulta nato il

Atto n. p.1 s.A u. 1

Motivo richiesta: t1

Ravenna , 06-07-2010

IL SINDACO

"Firma autografa sostituita ex art. 15 quinquies della Decreto-Legge 28/12/1989 n. 415 convertito con modifiche dall'art. 1 della Legge 28/2/1990 n. 38"

"Certificato emesso in conformità alle disposizioni del Ministero dell'Interno del 18/2/2009 PGN 0014674 depositate agli atti del Comune di Ravenna"

Firme automatiche

Art. 35, c.2 e c.3

- I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. **I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma** secondo quanto previsto dalle regole tecniche di cui all'articolo 71.
- Il secondo periodo del comma 2 **non si applica** alle firme apposte con **procedura automatica**. La firma con procedura automatica è valida se apposta **previo consenso del titolare all'adozione della procedura medesima**.

nuova dimensione

- L’impiego di questi strumenti produce effetti giuridici
- L’approccio deve pertanto essere diverso rispetto all’impiego di altri device … non sono una fidelity card !
- La rilevanza di tali strumenti dal profilo giuridico li rende ancora più appetitosi per i terzi malintenzionati
- Per questo, e ancora di più, l’approccio deve essere consapevole

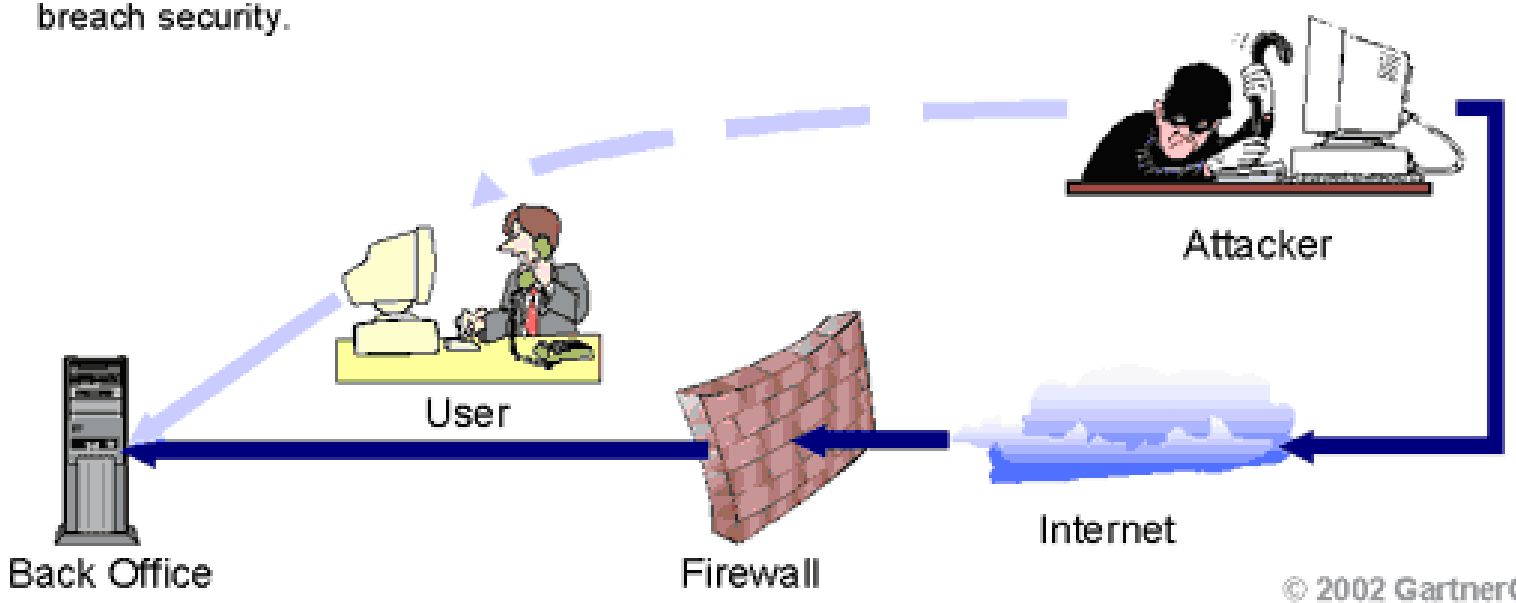
vulnerabilità e limiti

- Normativa
- Dispositivo di firma
- Certificatore
- Apparecchiatura del firmatario
- Software di apposizione della firma
- Fattore “U”

social engineering

Social Engineering

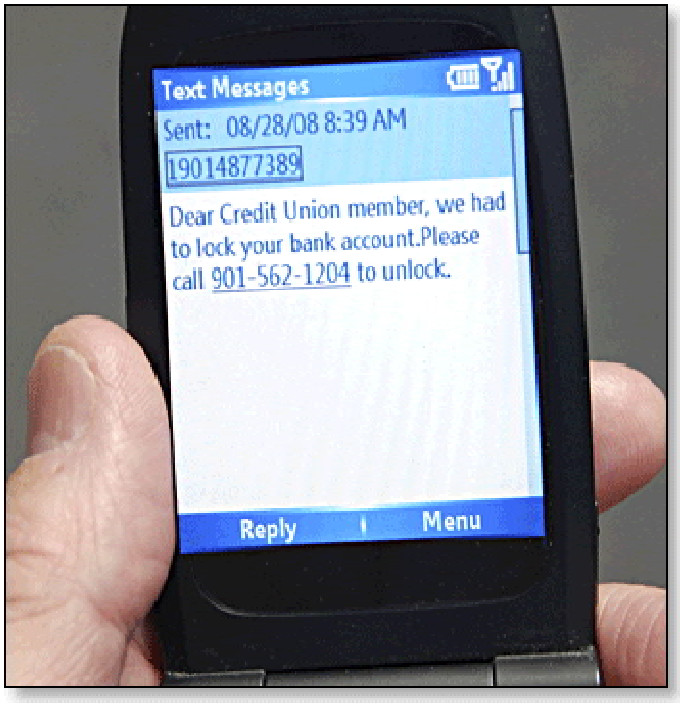
- Includes extensive research information (legal and illicit) about an enterprise, which is gathered and used to exploit people.
- Successful social engineering results in partial or complete circumvention of an enterprise's security systems. The best firewall is useless if the person behind it gives away either the access codes or the information it is installed to protect.
- Social engineering *principally* involves the manipulation of people rather than technology to breach security.



OpenSourceINTelligence

- è l'attività di raccolta di informazioni mediante la **consultazione di fonti di pubblico accesso**. Nell'ambito di operazioni di intelligence il termine "Open Source" si riferisce a **fonti pubbliche**, liberamente accessibili, in contrapposizione a fonti segrete o coperte.

phishing e smishing



dall’identità in rete al furto di identità

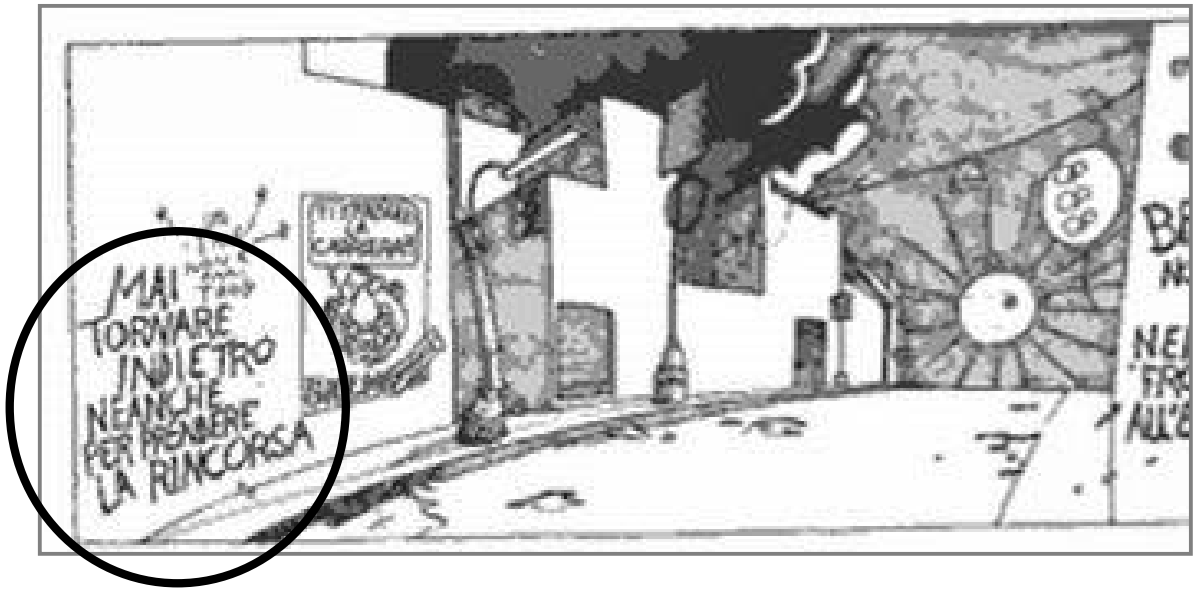
Art. 494 C.p. – Sostituzione di persona

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all’altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno.

conclusioni

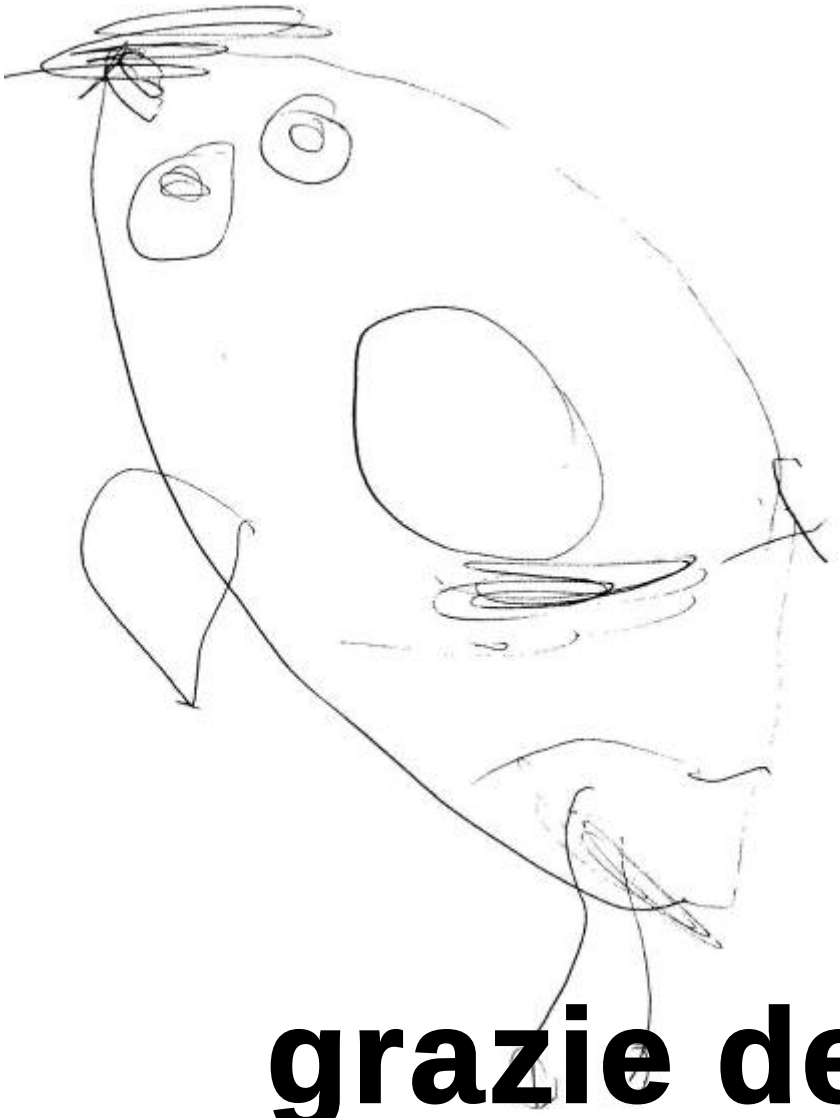
- L’identità in rete è un fatto!
- I dati che costituiscono e che sanciscono la propria identità in rete sono informazioni strategiche da preservare
- La normativa e la tecnica ci sono!
- Occorre consapevolezza e formazione anche sugli strumenti impiegati e sulle caratteristiche e i limiti di funzionamento
- E questo non solo nell’impiego ma anche nella impostazione delle strategie di innovazione
- Approccio consapevole e interdisciplinare

riflessione



MAI TORNARE INDIETRO NEANCHE PER PRENDERE LA RINCORSA

(Andrea Pazienza *riporta* Ernesto Che Guevara)



grazie dell’attenzione

michele[dot]**martoni**[at]**unibo**[dot]**it**